Risk Reduction using DDP (Defect Detection and Prevention): Software Support and Software Applications

Martin S. Feather
Jet Propulsion Laboratory, California Institute of Technology. Martin.S.Feather@Jpl.Nasa.Gov

Abstract

Risk assessment and mitigation is the focus of the Defect Detection and Prevention (DDP) process, which has been applied to spacecraft technology assessments and planning, both hardware and software. DDP's major elements and their relevance to core requirement engineering concerns are summarized. The accompanying research demonstration illustrates DDP's tool support, and further customizations for application to software.

The DDP Process: Dr. S. Cornford (JPL), creator of the DDP process, leads its development and application. DDP deals with the following elements:

Requirements – what the system hardware/software is to achieve. In DDP, requirements are weighted, reflecting their relative importance.

Failure Modes (FMs) – things that, should they occur, will lead to loss of requirements. In DDP, FMs can be given an a-prori likelihood (the chance of the FM occurring, if nothing is done to inhibit it).

"PACT"s – things that could be used to reduce the likelihood of failure modes and/or reduce their impact on requirements, namely Preventative measures, Analyses, process Controls and Tests. Each PACT has costs: budget, schedule, mass (for hardware), etc.

Impacts – for each Requirement x FM pair, how much of that Requirement will be lost should that FM occur

Effects – for each PACT x FM pair, how much of a mitigation that PACT will achieve against that FM.

Relevance of DDP to Requirements Engineering: The DDP process has been used on spacecraft project components and technologies, both hardware and software, to achieve the following benefits:

Elicitation – spacecraft typify projects in which expertise from multiple disciplines is combined. DDP supports the on-the-fly elicitation and capture of project-specific information, as well as use of pre-assembled knowledge bases.

Selection – since there are far more PACTs that could be done than there are resources to pay for them, their judicious selection must take into account costs and benefits. DDP's manipulation of quantitative data facilitates the cost-effective selection of PACTs. DDP also has been used to trigger and guide negotiation of requirements whose attainment is proving the most costly (i.e., require costly PACTs to reduce FM risks).

Assessment, Tailoring and Understanding – the net result of a DDP application is a tailored assessment of the project's risk profile, and an understanding of why activities are being done (namely, to mitigate the risks of specific FMs on requirements).

The net result: risk is traded as a resource.

DDP Tool: custom features that support: *Information capture and organization* in real-time; *Automatic calculation of derived information* pertinent to: requirements (for each requirement, how much at risk each it is), FMs (how much damage each is causing) and PACTs (how much benefit does each provide); *Cogent visualizations* that allow users to explore the risk, requirements and mitigations landscape; and *Decision support* that helps users in making choices.

Software-specific customizations: The DDP tool has been populated with information specific to software development efforts. In particular, best-practice knowledge drawn from the SEI: software development risks (in DDP, "FMs"), and CMM recommended activities (in DDP "PACTs"). The cross-linking of these (done by J. Kiper, U. of Miami, Ohio) captures knowledge of which activities address which risks – key to effective planning of cost-effective risk-reducing software developments.

The DDP tool has been augmented to interact with another NASA-developed tool, Ask Pete http://tkurtz.grc.nasa.gov/pete, in such a way that Ask Pete's capabilities to do estimation and planning feed as initial data into DDP for project-specific customization and cost/risk/requirements trades.

Finally, this version of the DDP tool is serving as a springboard for ongoing collaboration with other requirements research, including stakeholder-based negotiation (H. In, Texas A&M) and machine learning based search, optimization and sensitivity analysis (T. Menzies, U. British Columbia).

The research described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.